学校编码：10384　　分类号_____密级_____

学号：X2012230127　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

# 基于多协议标签交换的网络安全系统设计与实现

# Design and Implementation of Network Security System Based on Multi-Protocol Label Switch

李 澍

指 导 教 师： 姚俊峰 教授

专 业 名 称： 软 件 工 程

论文提交日期： 2016 年 1 月

论文答辩日期： 2016 年 3 月

学位授予日期： 2016 年 6 月

指 导 教 师：_____

答辩委员会主席：_____

2016 年 1 月

# 厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

2016 年　月　日

# 厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

2015 年　月　日

# 摘　要

VPN（虚拟专用网络）实例间隔离性出色是 MPLS（多协议标签交换）网络的一个重要特点，也正是由于这一优势，在最近几年，不同企业甚至不同行业间，均广泛采用这一网络。然而，VPN 实例内的安全性问题却没有进行充分的考虑。当前阶段中，通常将安全设备安装在 MPLS VPN 的网络边缘处，也就是 CE（用户边缘）设备部位，以达到保护的效果。然而，在网络的分支机构比较复杂的情况下，CE 设备也通常会随之增加，在这种情况下，利用这一方式通常需要支付较高的成本，而且不利于整网的实用性，同时，在后续维护和管理中也会带来较大的困难。因此，设计一个既能有效地针对 MPLS VPN 实例进行安全防护又能节省工程成本的安全解决方案非常有必要。

本文描述了如何在 BGP/MPLS VPN 网络环境中的 P（服务提供商）设备旁挂 UTM（统一威胁管理）设备，实现对 MPLS VPN 实例的安全防护，打破了目前常规的在 MPLS VPN 网络边缘处部署安全设备进行防护的做法。文中对系统需求进行详细分析，定义了系统设计目的、设计原则、用户角色、业务流程、功能性及非功能性需求，从原理出发设计了系统的实施环境，并对主要的几个原理进行详细解释，在之后的系统实现和测试中取得了预期的测试结果。文中首次提出利用 BGP（边界网关协议）路由协议的 local-pref 属性，实现 MPLS VPN 报文的引流、回注，同时利用路由策略防止环路的出现以及多个分支机构互访带来的各种问题，并在 UTM 设备上开启 IPS（入侵防御系统）、AV（反病毒）防护，实现整网的可用性和安全性的平衡。由于其已在全省性专用网络中得到应用，其将有很强的移植性和扩展性，并通过设备升级可平滑应对今后大数据时代下的安全威胁。

关键词：网络安全；多协议标签交换；边界网关协议

# Abstract

In recent years， MPLS (Multi-Protocol Label Switching) network has been widely applied in variety of enterprise and industry due to its characteristic of good isolation between the VPN (Virtual Private Network) instance. But MPLS VPN network security of VPN instance is not taken into consideration. The conventional solution is deploying security protection equipment at CE (Customer Edge) device，the edge of the MPLS VPN. But if it is large or medium-sized private network with numerous branches and a large number of CE devices， the conventional approach will lead to the high cost of implementation and difficulty of management and maintenance. Therefore， designing an effective solution which can not only carry out safety protection for a MPLS VPN instance but also save cost of the project is very necessary.

This paper describes that how to deploy UTM (Unified Threat Management) device hanging next to P (Provider) device in MPLS VPN network to achieve the security of VPN instance. It breaks the current conventional approach that security equipment's are deployed at the edge of MPLS VPN network. This paper gives a detailed analysis of the system requirement， defining system design objectives，design principles， user roles， business process， functional and non functional requirements of system design. It designs the implementation environment of the system according to the principle， giving the detailed explanation to several key principles. Finally it achieves the expected results in the next system implementation and testing. This paper first proposes the use of BGP (Border Gateway Protocol) attribute named local-preference to control the route of VPN packets ， taking advantage of the routing policy to prevent the emergence of loops and resolving the problems resulting from access of branches ， while using the function of IPS(Intrusion Prevention System) and AV (Anti-Virus) on UTM devices to achieve the balance of availability and security. Since it has been used in private network of some province， it has strong portability and scalability， and can smoothly deal with security threats in the age of big data through device upgrades in the future.

**Key words:** Network Security; Multi-Protocol Label Switching; Border Gateway Protocol

# 目 录

# Contents

# 第一章 绪论

## 1.1 研究目的及意义

伴随网络应用技术突飞猛进的变革，越来越多的应用借助于网络而得到长足的发展。而随着热衷及熟悉网络应用的70、80、90后们逐渐成为社会的主体人群，他们也更多的借助于网络平台来发表他们对社会、人生甚至信仰的看法。

然而，在这个开放及相对平等的虚拟世界里，各类观点的碰撞及利益等的冲突则是难以避免的。因此，基于网络发起的“战争”也就出现了。相对于一般网民的口诛笔伐，掌握一定网络技术的黑客群体显然更“黑”，他们无需现身亲力亲为，也不必发表过多的评论，但却在一次次的网络事件充分体现了他们的“观点”或意志，得到他们希望获取的利益。

部分黑客借助自己的技术获取灰色甚至黑色的收入，或者通过网络攻击对特定主体表达他们的不满。在这些非法活动中，游戏运营商、网络服务提供商、网络运营商及政府网站等往往成为入侵、攻击的主要对象。部分社会活跃名人也可能成为了黑客特别“关照”的重点[4]。

无论是社会稳定的维持，还是民族文化的集成和发扬方面，甚至在国家安全和主权的问题上，网络安全都扮演了炙手可热的重要角色。目前，信息化应用在世界范围内呈现出如雨后春笋般的生机勃勃，同时，网络安全的重要性也表现的尤为突出[13]。

网络安全实质上指的是在网络环境中信息的安全性，无论是网络系统的软件部分还是硬件部分，甚至系统内的所有相关数据都能够得到有效的保护，其在运行过程中不会受到恶意侵袭或者某种偶然因素所所造成的破坏或泄露等现象，从而确保网络服务的持续性。网络安全通常会涉及到多种不同的学科，例如计算机科学、通信技术、信息安全技术，又如网络技术、应用数学，信息论等，因此，其是一门综合性较强的学科。基于这一分析，无论是信息的保密性、真实性，还是信息的完整性、可控性等，其都可以归纳为网络安全的研究领域[7]。

一般情况下，基于不同的视觉来分析，网络安全的含义通常会发生变化，主要有下列几种：

第一，基于用户或企业、个人视觉出发，为了能够有效的维护个人隐私、商业利益等相关信息不被外界恶意篡改或窃取，信息在网络传递过程中应充分考虑

机密性、安全性及完整性[14]。

第二，基于网络运行和管理者这一视觉出发，在进行本地网络信息的访问或读写等程序中，通常会受到关注，以便于信息能够得到有效的保护和控制，从而能够预防信息被黑客或病毒等攻击、非法占有或威胁等[12]。

第三，基于安全保密部门这一视觉出发，这类部门通常比较关注国家机密信息的安全性，因此，网络安全能够有效的堵截那些恶意或非法信息，从而能够规避网络风险的发生，进而维护国家的利益。

第四，基于社会教育、意识形态这一视觉出发，通常比较关注网络环境中涉及到的各种内容是否能够对社会稳定产生不利影响，对给人类进步带来不利的内容进行控制[11]。

VPN实例间隔离性比较良好是BGP/MPLS VPN网络的一个重要特点，在最近几年，不同企业甚至不同行业间，均采用这一网络。然而，VPN实例内的安全性这一问题却没有在该网络中有效体现，在网络体系中，如果病毒入侵到一台设备中，通常会在VPN实例中快速进行传播。当前阶段中，通常将安全设备安装在MPLS VPN的网络边缘处，也就是CE设备部位，以达到保护的效果。然而，在网络的分支机构比较复杂的情况下，利用这一方式通常需要支付较高的成本，而且不利于整网的实用性，同时，在后续维护和管理中也会带来较大的困难[8]。

## 1.2 国内外发展现状

无论是VPN运营商还是客户，安全性问题均受到了他们广泛的关注，当然，有学者和专家也曾指出，在BGP/MPLS VPN网络中，这一问题是其最大的弱点。通常来讲，我们可以从三个层面对安全性分型分析，一是数据平面的安全；二是控制平面的安全；三是设备安全[1]。

1.数据平面

数据平面安全性通常需要进行两方面的保护，一是当VPN内的包向其之外的站点进行传递时，需要按照该VPN站点的要求进行；二是当一个外部的数据包进入到某一VPN站点时，需要按照该VPN的要求进行。然而，会存在下列几种现象：

(1) 通常情况下，骨干网路由器不会来自特定链路上的受标记的包。并不从特定链路上接受标记后的包，除非它知道该数据链路只连接到了它值得信任的网络，

(2) 但也存在例外情况，如骨干网路由器已经确认这些数据链路仅连接了信任网络，不存在安全问题。

(3)这些数据包接收后仅进行简单操作即会离开骨干网，如检查 IP 头、低层次标记等。不从不可靠或有嫌疑的路由对等体接受标记后的 VPN-IPv4 路由，且没有在控制平面成功安装攻击机制。

基于这些现状，该机制通过数据平面这一体系所提供的安全性，实际上可以表现为 FR 或 ATM 骨干网所提供的安全性。一旦我们将运营商所控制的设备进行了有效的配置，在得不到相应授权的前提下，数据是无法进入 VPN，同样的，数据也无法离开 VPN。

2.控制平面

基于这些现状，该机制通过数据平面这一体系所提供的安全性，实际上可以表现为 FR 或 ATM 骨干网所提供的安全性。一旦我们将运营商所控制的设备进行了有效的配置，在得不到相应授权的前提下，数据是无法进入 VPN，同样的，数据也无法离开 VPN[2]。

3.P 和 PE 设备的安全性

一旦出现设备物理安全性受到严重破坏的情况，数据平面的安全性通常会无法得到有效的保护，在常规方式中，公开 Internet 的 IP 流量通常不会对设备配置进行篡改，此外，也可以通过安装 DOS 攻击来对其进行保护。

## 1.3 应用前景

MPLS 也被称为多协议标签交换，是在 VPI/VCI 交换思想的基础是哪个形成的一种新的基础，将 IP 路由技术的灵活性充分发挥并且结合了两层交换的特点，这种技术的出现对 IP 网络中面向连接属性的实现有重要推动作用。在多协议标签交换技术中采用的虚拟连接方式具备一定的优势，能够增加 IP 运营和管理的手段和途径。MPLS 技术的应用得到了普及，尤其是伴随着科学技术的不断发展流量工程成为了技术发展的主要方向，为网络协议技术发展指明了道路。MPLS 是一种在网络中使用的流量工程技术，这种类型的技术包括了流量管理，并且在一定程度上促进了 QoS 的发展，对于解决网络上存在的拥堵现象有重要意义。MPLS 能够提供各种新的业务类型，成为了网络业务发展和增殖价值实现的关键

措施。

IGP/BGP 是 IP 网络中使用最广泛的协议类型，尤其是 OSPF 协议发挥了主要作用，在很多大型的网络体系中得到了广泛应用。协议简单和面向对象无连接性是 IP 路由器的重要特征，最重要的是采用新的协议技术能够防止故障发生时出现影响网络速度和正常连接的弊端。在 IP 网络连接的过程中最先考虑的是网络连接的问题，为了确保网络的顺畅性并没有充分考虑 QoS 的作用，而在现实情况下 IP 网络必须解决QoS 带来的一系列的问题，一般而言我们最常见的解决方式是采用 MLPS 流量技术提供保障。

MPLS 流量工程技术表示的是在网络中建立一种调节模式，在全网络的范围内进行流量调节和整合从而促进网络流量的均衡发展。一般在网络发展的过程中存在超负荷和流量衔接不足的两种极端现象，因此必须在建立网络流量 LSP 的基础上对流量进行调节和均衡处置，这样就能够将负荷量大的链接向负荷量小的链接上进行转移，从而实现网络流量发展均衡的最终目标。MLPS 流量工程的建设对于宽带约束有重要意义，实现了 LSP 建设符合相关要求，对 MLPS 流量建设符合宽带要求有重要作用。

在 MLPS 的支持下可以实现对 LSP 的抢占，提高了宽带的使用率和重要用户的抢占，因此我们可以提高其抢占级别并且在其他 LSP 资源中得以体现。LSP 能够抢占一些重要级别较低的市场，以其为基础建立市场之后不希望被它抢占市场。

MLPS 流量工程一般来说能够拥有 8 个以上的级别，并且保持每个级别的链条上都能被标示并且开展相关业务，可以用其进行地理位置的标识或者开展 Voip 业务。在 LSP 建立的过程中能够确保在一个区域内的 LSP 不会超出本区域内影响业务发展[3]。

## 1.4 论文研究内容

转发特性是 BGP/MPLS VPN 网络的重要特征，此外在各个实例中存在一定的间隔性也是该网络体系特征的重要表现类型。业界对于 VPN 网络中的安全性保证一般采用的是在 VPN 实例中具体解决的方法。VPN 保护的实例在网络上实施的安全防护措施一般是在 CE 设备的位置安装相关防护，而针对大型的网络或